Free Questions for GSEC by vceexamstest

Shared by Heath on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Which of the following is the key point to consider in the recovery phase of incident handling?

Which of the following is the key point to consider in the recovery phase of incident handling?

Options:

A- Isolating the source of the compromise

B- Shutting down the system

C- Ensuring that vulnerable code is not being restored

D- Preparing the jump bag

Answer:

C

Question 2

Question Type: **MultipleChoice**

How does a default deny rule in a firewall prevent unknown attacks?

Options:

A- Slops users from clicking on known bad URIs.

B- Forbids outbound access with unknown payload.

C- Blocks packets that are not explicitly allowed.

D- Refuses packets that match a defined set of rules

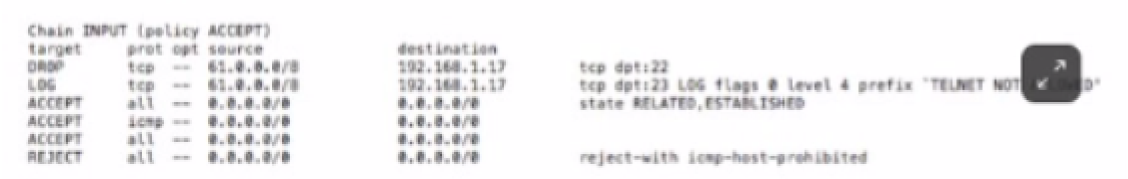
Answer:

C

Question 3

Question Type: **MultipleChoice**

Based on the iptables output below, which type of endpoint security protection has host 192.168.1.17 implemented for incoming traffic on TCP port 22 (SSH) and TCP port 23 (telnet)?



```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  61.0.0.0/8           192.168.1.17         tcp dpt:22
LOG        tcp  --  61.0.0.0/8           192.168.1.17         tcp dpt:23 LOG flags 0 level 4 prefix 'TELNET NOT [illegible]D'
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
REJECT     all  --  0.0.0.0/0            0.0.0.0/0            reject-with icmp-host-prohibited
```

Options:

A- Operating System Control Firewall

B- Application Control Firewall

C- Exclusive Logging Analysis

D- Packet Filtering Firewall

E- Application Execution Control

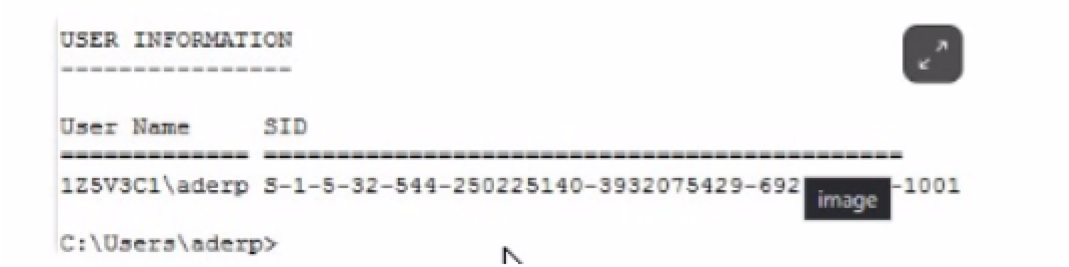
Answer:

A

Question 4

Question Type: MultipleChoice

Analyze the following screenshot. What conclusion can be drawn about the user account shown?



```
USER INFORMATION
----------------

User Name     SID
============= ============================================
1Z5V3C1\aderp S-1-5-32-544-250225140-3932075429-692 image -1001

C:\Users\aderp>
```

Options:

A- The user is a domain administrator

B- The user has a guest privilege level

C- The user is a local administrator

D- The user is not authenticated on the domain

Answer:

C

Question 5

Question Type: MultipleChoice

An application developer would like to replace Triple DES in their software with a stronger algorithm of the same type. Which of the following should they use?

Options:

A- RC5

B- AES

C- RSA

D- SHA

Answer:

B

Question 6

Question Type: **MultipleChoice**

What security advantage does the utilization of a switch as opposed to a hub offer for a secure network design?

Options:

A- A switch will make it possible to provide a physical separation of the cables used to connect systems to the network.

B- A switch will make it more difficult for an attacker that may control a compromised system to be able to view traffic destined for other devices on the same logical network.
A switch will make it easier to deploy Intrusion detection or intrusion prevention systems as a method of providing an additional layer of security to a proper secure network design.
A switch will remove the need for utilization of a host-based firewall.

Answer:

B

Question 7

Question Type: **MultipleChoice**

What method do Unix-type systems use to prevent attackers from cracking passwords using pre-computed hashes?

Options:

A- Unix systems can prevent users from using dictionary words for passwords

B- The algorithms creates hashes using a CPU- intensive algorithm.

C- The algorithm creates hashes using salts or randomized values

D- Unix/Linux systems use hashing functions which cannot be reversed

E- The system encrypts the password using a symmetrical algorithm

Answer:

C